Candid Camera: Nobody's Laughing Anymore!

Face Recognition Technology as a Law Enforcement Tool

By Darryl McAllister

For many of us, it feels like it was merely yesterday when the hit 1950's television show, Candid Camera, took America by storm. Week after week, men, women, boys and girls were wooed into their living rooms and captivated by scenarios in which unwitting members of the public would be placed in outlandish situations for our laughter and entertainment. The victim of the prank's reactions would be filmed by a concealed camera, and at some stage the joke is finally revealed to them, when the victim would be told "Smile, you're on *Candid Camera*!"

In the entertainment world, the concept of capturing the public's face on camera seems to have evolved to the point where the intrigue is much less about the situational storyline of the video and much more about its technological prowess. Under the umbrella of "special effects," Hollywood continues to captivate people's imaginations of the future by glamorizing sleek video identification technologies as an element of everyday life. From movies such as *Mission Impossible* and *Enemy of the State*, to television shows such as *CSI*, *24*, and *Las Vegas*, hardly a storyline comes out of Hollywood that doesn't feature face recognition technologies. These entertaining concepts have contributed a great deal to the world of science fiction and fanciful imagination, but the reality is face recognition technology—a form of biometrics—is rapidly growing as a viable tool for real-world issues such as public safety and security.

BIOMETRICS AND FACE RECOGNITION

The term "Biometric" encompasses the words "biology" and "measurement." It is one of several technologies intended to identify individuals using the body's immutable physical characteristics. In addition to face recognition systems, there are fingerprint readers, iris scanners, voice analyzers and even computer-linked cameras that recognize the way people walk.[1] Accompanying that growth is a new demand for law enforcement to understand, embrace, and ultimately use face recognition and other biometrics for public safety and information security. There is also no doubt the emergence of this controversial technology raises ethical questions and concerns about policing's eventual use of face recognition for criminal investigations and covert operations as well.

HOW IT WORKS

A face recognition biometrics system analyzes the characteristics of a person's facial image as captured by a digital video camera or similar means. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera. Face recognition technology analyzes the characteristics of a person's face images input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used for comparison.[2]

---

[1] Christian Parenti, "The Soft Cage: Surveillance in America", (New York: Basic Books, 2003), 158

[2] Facial Recognition (2002), National Center for State Courts [online] accessed May 21, 2006, available: http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html

What sets face recognition technology apart from other biometrics is it can be used for surveillance purposes. Unlike iris scans, hand geometry, fingerprint recognition, or voice recognition, face recognition does not require close proximity to the donor for purposes of identification. Face recognition technology, therefore, can be used without the subject ever knowing he or she is the focus of such a scan. This opens the door to a host of considerations and uses, particularly in intelligence and covert operations.

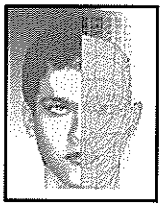
The distinctions are subtle yet compelling to justify the use of face recognition technology. In making the distinction, law enforcement must decide whether it will use the technology for verification versus identification purposes. Verification implies face recognition biometrics will be used to answer the question, "Is this that person?" after the person claims to be a particular identity. Identification, on the other hand, implies the technology will be used to answer the question, "Who is this?" by reading a facial sample and comparing that sample against a database.

HISTORICAL PERSPECTIVE

Face recognition biometrics is rooted in concepts dating back to the late nineteenth century to the Bertillon system of measurement. Pioneered in the 1880s by Parisian anthropologist Alphonse Bertillon, the system relied on a belief that a person's bone structure remains unchanged after age twenty. Bertillon focused much of his work on shape and breadth of the head and face. Suspected criminals were relegated to a physical exam during which their head and body measurements were recorded and manually compared to Bertillon's elaborate cataloging system. Though done by hand, the record filing and checking system was quite fast

for its time.[3] Bertillon's system spread to world-wide use for more nearly two decades until the system was derailed by inconsistent measurements of the same people, resulting in misidentifications and the jailing of the innocent. The Bertillon system was summarily discredited and abandoned in favor of discoveries in fingerprinting.[4]

Computer vision technology was born in the late 1950s, using rudimentary programming to detect images. Through the 1960s and '70s, experts increasingly experimented with new ways to enhance the computer's ability to distinguish one image from another, eventually spawning the growth of face recognition biometrics. The watershed breakthrough came in the late 1980s with the influx of eigenface algorithms in face recognition computing.[5] Eigenfaces are statistical analyses of multiple facial images. Using algorithms, one image of a human face can be mathematically compared to a combination of the pictures; a subject's face might compare 10% to one picture, 24% to another picture, and so on.[6]



American use of public video surveillance lags far behind that of European countries such as Britain, where public video surveillance is the single most heavily funded non-criminal justice crime prevention measure.[7] Many British residents go about their daily lives like

---

[3] Bertillonage (2002), National Center for State Courts [online] accessed June 11, 2006, available: http://ctl.ncsc.dni.us/biomet%20web/BMBody.html

[4] Alphonse Bertillon (2006), Wikipedia Encyclopedia, [online] accessed June 11, 2006, available: http://en.wikipedia.org/wiki/Alphonse_Bertillon

[5] The History of Face Recognition (2005), Riya Beta PhotoSearch, [online] accessed June 11, 2006, available: http://www.riya.com/historyFaceRecognition

[6] Eigenface (2006), Wikipedia Encyclopedia, [online] accessed June 11, 2006, available: http://en.wikipedia.org/wiki/Eigenface

[7] Welsh, Brandon C., Farrington, David P., Effects of Closed Circuit Television Surveillance on Crime (2003), Campbell Collaboration Crime and Justice Group [online], accessed June 12, 2006, available: http://www.campbellcollaboration.org/doc-pdf/cctv.pdf

contestants in a reality-TV show; a substantial network of public cameras track their every move on residential and commercial streets, on buses, trains and subways, in offices, pubs and malls, even in churches and schools. Experts calculate the average commuter in London is filmed 300 times each day.[8] Canada began using video surveillance on public streets and areas only five years ago, while recent terrorist activity prompted the French government to permit its police to use electronic surveillance in public places. Spain and Italy have followed suit, identifying the need to increase video surveillance to better monitor public areas and high-profile buildings. Ireland and Russia have been using public surveillance cameras for decades but are encouraged to do even more because of advances in face recognition technology.[9]

Most Americans first heard about face recognition biometrics after the September 11th terrorist attacks, even though football fans had been scanned en mass at Super Bowl XXXV in Tampa, Florida months earlier.[10] The concept has since gained support as a potential tool for averting terrorist crimes, but still, the application of face recognition biometrics for local law enforcement is an issue of intense debate.[11] Face recognition technology is far from widespread use, with the scales tipped heavily toward federal use for national security issues. Only recently has this technology been applied to local law enforcement investigations on a very limited basis and is therefore a virtually untapped resource for the future.

---

[8] Britain's Big Brother (2003), Free Speech [online] accessed June 12, 2006, available: http://www.freespeech.com/archives/002424.html

[9] Nieto, Marcus; Public Video Surveillance: Is it an Effective Crime Prevention Tool? (1997), California Research Bureau [online], accessed June 12, 2006, available: http://www.library.ca.gov/CRB/97/05/crb97-005.html#public

[10] Superbowl Face Scan (2001), Wired News [online] accessed May 21, 2006, available: http://www.wired.com/news/politics/0,1283,41571,00.html

[11] Facing A Harsh New Surveillance Reality (2001), John Jay College of Criminal Justice Law Enforcement News [online] accessed May 21, 2006, available: http://www.lib.jjay.cuny.edu/len/2001/12.31/facing.html

Although unproven as an accurate and effective way to identify terrorists or wanted suspects, some of the proposed post-September 11th uses of the technology—such as in

immigration and airport security—have been welcomed by the general public. Before the September 11 attacks, the public viewed with skepticism the notion public cameras could be used for advanced technologies such as face recognition. Though skepticism has given way to rising fears about terrorism, many are still wary of widespread public use of the technology. People are most concerned about the risks of identity theft and privacy infringement.[12]

THE ADVANTAGES

A strong positive aspect of face recognition technology is its non-intrusive method to conduct an investigation. Verification or identification can be accomplished from as few as two feet away or from a significant distance with appropriate lenses. In situations where cameras are covertly placed, the subject's freedom of mobility is unhindered. Law enforcement has at its disposal the potential for finding fugitives and collecting vast amounts of intelligence information to bolster the quality and expedience of investigations. With well-placed cameras and face recognition technology as primary tools for investigating local crime, law enforcement's ability to prevent crime would likely soar because of the ability to identify, ahead of the crime, individuals whose criminal history suggest a particular propensity. At the local level, face recognition technology could be a hugely effective tool to investigate

Law enforcement has at its disposal the potential for finding fugitives and collecting vast amounts of intelligence information to bolster the quality and expedience of investigations.

[12] Face recognition Systems (2003), Forensic-Evidence.com [online] accessed May 22, 2006, available: http://www.forensic-evidence.com/site/ID/facialrecog.html

identity theft—one of the fastest growing crimes everywhere. Face recognition applications are an obvious antidote to identity theft because of the potential to harden our information security environment by making it more difficult for criminals to impersonate other's identities.

Although there are no verified success stories on behalf of this biometric technology's effectiveness, many facial identification advocates say the cameras have not caught any suspects because they have successfully deterred terrorists and other criminals from entering the protected areas.[13]

THE CHALLENGES

Of all the biometric technologies currently in use, face recognition is arguably the most controversial. It can be deployed as an exceptionally pervasive surveillance means, and will earn your attention with its potential to integrate with other biometric and authentication applications such as smart cards and digital signatures.[14] Civil libertarians and privacy advocates are certainly not comfortable with the emergence of face recognition technology as a law enforcement investigative tool. According to a 2003 RAND report, many Americans feel the technology amounts to improper, random mass scanning and law enforcement, bound by the Fourth Amendment, must first have individualized, reasonable suspicion of criminal activity before it can "search" someone's face to see if it matches that of an individual in the database.[15] In a prior ruling, the United States Supreme Court disagreed, citing a person does not have a

[13] Face Recognition Systems (2003), Forensic-Evidence.com [online] accessed May 23, 2006, available: http://www.forensic-evidence.com/site/ID/facialrecog.html

[14] Does Facial Recognition Have a Future? (2002), Intelligent Enterprise [online] accessed May 23, 2006, available: http://www.intelligententerprise.com/020416/507bus_impact1_1.jhtml

[15] Woodward, John; Gatune, Julius, "Biometrics: A Look at Facial Recognition", (Santa Monica, California; RAND, 2003)

reasonable expectation of privacy in those physical characteristics constantly exposed to the public, such as one's facial characteristics.[16]

The non-intrusiveness of face recognition technology, mentioned earlier as an advantage to law enforcement, is also a drawback when it comes to public opinion. Many people have expressed concern about face recognition cameras placed inconspicuously around cities attempting to identify passers-by without their knowledge or consent.[17] Some opponents say the potential for abuse is astronomical and cameras could easily be networked to track individuals from place to place, thus enabling the government to monitor individuals for social control. Individuals might be less likely to contemplate public activities offensive to powerful interests if they knew their identity would be captured on video and made accessible to opposing interests.[18] People simply fear face recognition technology will become an errant tool for government to capriciously and arbitrarily cross the line, thus invading the privacy of individuals. Many are concerned that from the moment they step out of their home until the time they return, cameras will track their every move, read what they're reading, know what they're eating and who they're spending time with, making each person wary of their surroundings and less likely to feel free. Opponents point out that face recognition systems are operated by humans, who bring to the job their existing prejudices and biases.[19] One such example is the potential to use face recognition to augment perimeter cameras around certain buildings, such as welfare offices or

---

[16] *United States v. Dionisio*, 410 U.S. 1 (1973).

[17] Facial Recognition (2002), National Center for State Courts [online] accessed September 4, 2005, available: http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html

[18] Thomson Gale, "The War on Terrorism: Opposing Viewpoints", (Farmington Hills, Michigan: Greenhaven Press, 2005) 151

[19] Thomson Gale, "Civil Liberties: Current Controversies", (Farmington Hills, Michigan: Greenhaven Press, 2003), 136

public assistance centers. Some argue this would tempt its use as an enforcement tool, since some of the disadvantaged might be more likely to have criminal records.

Advocates of face recognition disagree about the threat to personal privacy the opponents claim is in jeopardy. Proponents argue there is no constitutional right to privacy in the face we show in public. They point to the fact the United State Supreme Court has determined government action constitutes a "search" when it invades a person's reasonable expectation of privacy. This legal standing, according to proponents, explicitly provides that a person does not have any reasonable expectation of privacy in those physical characteristics constantly exposed to the public, such as one's facial features, voice, and handwriting. Therefore, although the Fourth Amendment requires a "search" be reasonable, the argument is the use of public cameras for face recognition does not constitute a search, and the government is not constrained from employing face recognition systems in public spaces.[20]

In its current state, face recognition technology has experienced some setbacks. Despite vehement protest by the American Civil Liberties Union, the City of Tampa, Florida became the first city in the United States to install the technology in June 2001 to scan faces in the city's nightlife district and check them against a database of more than 24,000 felons, sexual predators and runaway children. A police officer remotely monitored video images, and could select faces in the crowd to scan and run through a criminal database to search for matches. Tampa officials faced a deluge of criticism from residents and public interest groups objecting to the notion of monitoring of ordinary citizens in public places. Protesters donned bandanas, masks and

[20] Thomson Gale, "The War on Terrorism: Opposing Viewpoints", (Farmington Hills, Michigan: Greenhaven Press, 2005) 147

Groucho Marx glasses, taking to the streets of City's Ybor District on a busy Saturday night to show their contempt for the face-scanning system.[21] Over a two-year period, the system failed to deliver a single match and the city is at a loss to explain why the software wasn't effective (despite successful controlled testing). Yielding to failure, the Tampa Police Department finally decided to scrap its face recognition system in August 2003.[22]

Virginia Beach was the second U.S. to install a face recognition system on its public streets. In 2002, several closed-circuit cameras were installed to provide a visual canvass of the city's boardwalk.[23] Similar to the experience in Tampa, it too suffered from disappointing results. More than a year after its 2002 installation, the system failed to produce a successful identification or arrest. The Virginia Beach system is still up and running and officials say the cameras serve as a deterrent to criminals. They also decline to state where the video cameras are located and which are equipped with face recognition software.[24]

Of course, just because face recognition technology has had a rough start does not mean it will never work. Face recognition companies are receiving massive amounts of corporate

[21] Ybor Cameras Won't Seek What They Never Found (2003), St. Petersburg Times [online] accessed June 11, 2006, available: http://www.sptimes.com/2003/08/20/Hillsborough/Ybor_cameras_won_t_se.shtml

[22] Tampa Police Eliminate Facial-Recognition System (2003), Atlanta Journal Constitution [online] accessed May 24, 2006, available: http://www.ajc.com/news/content/news/0803/21tampacams.html

[23] Virginia Beach Installs Face-Recognition Cameras (2002), The Washington Post [online] accessed June 11, 2006, available: http://www.washingtonpost.com/ac2/wp-dyn/A19946-2002Jul3

[24] Face Recognition cameras a flop in Virginia Beach (2003), Privacy Activism [online] accessed June 11, 2006, available: http://www.privacyactivism.org/Item/168

funding in addition to tens of millions of dollars they receive from the Departments of Justice and Defense, respectively, for research and development.[25]

Even if corporate research and development of face recognition technologies is enough to spawn its use by law enforcement, though, the same typical barriers to innovation remain. The expense of new technologies includes both the cost of procuring it as well as the costs associated with maintaining and refining the application. And, as in the case of local law enforcement, the ability to shoulder those costs is predicated by the extent to which the taxpaying community is supportive of the endeavor. A community wary of facial biometrics may create challenges for local law enforcement to embrace it as a tool.

PREPARING FOR THE IMPACT

It is clear biometric face recognition applications have the potential to provide significant benefits to law enforcement's investigative arsenal, while at the same time, future growth and improvement in the technology could also threaten individual privacy rights.[26] Balancing individual privacy against law enforcement's need to investigate is a regular occurrence likely to become trickier with the emergence of biometric face recognition as an investigative tool. The debate is ferocious, and it is clear the accelerated focus to use public cameras for face recognition biometrics has been forged by the backdrop of terrorism and other world events. We cannot say for certain the technology will proliferate to widespread use in the coming years, but American law enforcement is forced by world trends to incorporate a global perspective into its localized view of crime. The potential widespread implementation of face recognition

[25] Thomson Gale, "Homeland Security", (Farmington Hills, Michigan: Greenhaven Press, 2004), 82
[26] Thomson Gale, "Civil Liberties: Current Controversies", (Farmington Hills, Michigan: Greenhaven Press, 2003), 141

technology is simply a tool of that endeavor. It is by no means a perfect technology and a great deal has to be done before it becomes a truly viable tool to investigate crime. The technology is getting better, however, and there is no denying its tremendous potential.[27]

Despite all the hoopla about the debacles in Florida and Virginia, it seems evident face recognition technology has gained the requisite momentum to forge ahead until it finds consistent success. Just as America has wholly embraced face recognition in action-packed movies and television shows, many agree real-life acceptance of the technology is simply a matter of time. Set aside for a moment the concern about the costs of face recognition systems. According to the San Jose, California-based U.S. National Biometrics Test Center, the biometrics market rose from $6.6 million in 1990 to $63 million in 1999, and is expected to eclipse $520 million by 2006 the end of 2006.[28] This type of exponential growth speaks to the basic laws of supply and demand. Considering the Federal Government's keen interest in proliferating face recognition biometrics as a tool to combat terrorism, local governments are poised to receive the help they need to handle the cost of implementation as the cost of acquiring and using such systems continues to fall. The U.S. Department of Defense already funds more than $50 million for university research to improve the technology.[29] And although social opposition may continue, one can argue the success of face recognition systems in the private sector is the best predictor of future success of public applications of the technology.

---

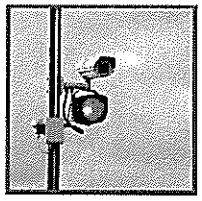
[27] Thomson Gale, "Homeland Security", (Farmington Hills, Michigan: Greenhaven Press, 2004), 83

[28] Face Recognition Tech Has People Pegged (2001), Cable News Network [online], accessed June 13, 2006, available: http://archives.cnn.com/2001/TECH/ptech/07/17/face.time.idg/

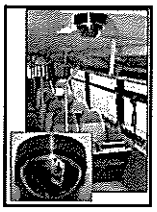
[29] Scheeres, Julia; Smile, You're on Scan Camera (2002), Find Biometrics [online], accessed June 13, 2006, available: http://www.findbiometrics.com/Pages/smile.html

Industry insiders rave about how face recognition software is often compatible with the computers and cameras already in use by airports, banks, casinos and other corporations.[30] The operation of these private systems has become a matter of routine, and conventional wisdom suggests the same will be true if public surveillance cameras proliferate throughout out cities. Consider how the added scrutiny at American airports has become more of an accepted reality than a dreadful intrusion. It seems equally plausible Americans would grow accustomed to the idea of public cameras as a measure of security and as a crime fighting tool. In the meantime, law enforcement must plan for the continued emergence of this new technology as a possible mandate for the future of public safety.

So, when you finish reading the last words of this article, you are challenged to lift your eyes, look around and ponder whether there is a camera capturing your face. If you're reading this while on a commercial aircraft, ask yourself if the candid camera is watching you; after all, *Airbus*, one of the leading manufacturers of commercial aircraft has already installed hidden security cameras in the light fittings above the seats in many of its planes.[31] Or maybe you're in



your car, stopped at a red light, trying to catch the last paragraph before the light changes. Is there is a traffic camera measuring your facial image in case you run the light? If you're reading while using public transportation,



take a glance; is there a camera peering at you and the other passengers on your bus, train, taxi or limousine? Did you know security cameras such as Mobile Digital

[30] Jarvis, Angela; Facial Recognition Systems: Are Privacy Rights of Citizens Being Eroded Wholesale? (2003), Forensic Evidence [online], accessed June 13, 2006, available: http://www.forensic-evidence.com/site/ID/facialrecog.html

[31] Hidden cameras to monitor aircraft passengers (2002), New Scientist [online] accessed June 1, 2006, available: http://www.newscientist.com/article.ns?id=dn2256

Video Recorders have been widely used in taxi cabs, buses, police cars and other public vehicles?[32] Perhaps you're in a waiting room somewhere—or in any public or private building for that matter. Chances are you can scan for a security camera and find it staring back at you. Ponder the notion many of the cameras around us, if not already tied to a face recognition system, provide a universal infrastructure for the proliferation of face recognition biometrics as a measure for public security and law enforcement investigation.

One thing is for sure: The laughter about Candid cameras of the 1950s pales in comparison to the debate about the covert cameras of today. We're certainly still captivated, but nobody is laughing anymore. Whether you support or oppose the use of public cameras for face recognition biometrics, it would nonetheless behoove you to smile—wherever you go.

[32] Mobile DVRs (2006), Security Camera World [online] accessed June 1, 2006, available: http://www.securitycameraworld.com/mobile-dvrs.html

About the Author

Darryl McAllister is a Captain and 23-year veteran with the Hayward, California Police Department. He holds a Bachelor's Degree in Occupational Studies from California State University, Long Beach and has also served as a credentialed Criminal Justice Instructor at the high school level. Captain McAllister recently conducted a research project on Face Recognition Biometrics while attending the California Command College, certified by the California Commission on Peace Officer Standards and Training.